LifeSkills

Financial fraud, scams and identity theft

Age range: 16+

Barclays LifeSkills have partnered with Spectra First to support those leaving care to build their employability skills and financial capability. As a signatory of the **Care Leaver Covenant**, alongside other organisations, Barclays has committed to offer a different type of support and expertise from that statutorily provided by local authorities. For more information visit mycovenant.org.uk.

Pages 1-2 of this pack are delivery notes for the facilitator, and pages 3-6 are worksheets for young people. Page 7 has a list of links for further support.

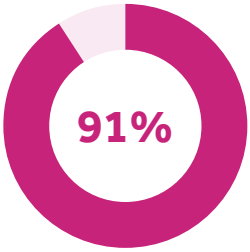
Financial fraud statistics

10 mins

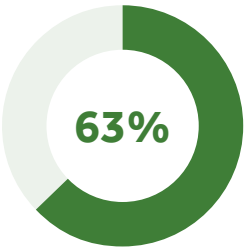
Ask the group/individual whether they have heard of any financial risks or types of fraud.

- Most of the time these involve fraudsters obtaining personal details and using these to open bank accounts or make purchases in that person's name, or tricking people into transferring money into a fake account
- Run the group/individual through the below stats. You could ask them to guess the percentage for each fact in a quiz-style format. These stats can also be found on **Worksheet 1**

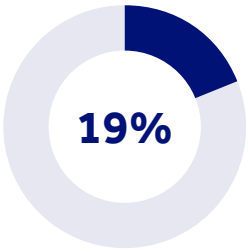
In 2021



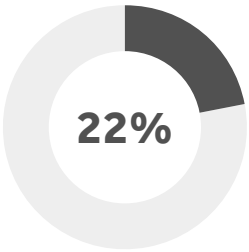
of identity fraud was committed online



of all fraud is identity theft



increase in identity theft among those under 21 since 2020



growth in identity fraud cases in 2021

Source: [Cifas Fraudscape Report 2022]

- Ask the group to discuss how using social media could put them at risk of identity theft. Ask for examples – these could include geo-tagging photos that give away their home address, fraudsters creating copycat accounts using their name and profile picture etc.

What are the consequences? How could they avoid this sort of fraud happening?

- Cifas have produced an engaging short film (1 min 30 secs) which exposes how much personal information is accessible to fraudsters via our social media accounts. Show this film by searching online for 'Cifas data to go'. Ask why they think they should be careful about the information they share publicly
- Summarise the video by reminding the group/individual that they should check how much personal information is public on their social media accounts, e.g. birthday, home town, pet names, holiday dates, job title. Fraudsters can use this information to steal a person's identity and apply for bank accounts or buy products in their name

LifeSkills

Financial fraud, scams and identity theft

Understanding frauds and scams

20 mins

- You may want to discuss the following terms together using **Worksheet 2**, before looking at the case studies. Explain that in many instances when you are taken advantage of, provided you have followed all the rules for use of your account, the bank or financial institution may help to return any lost funds to you

Vishing: A phone call from a fraudster posing as an employee of a reputable company or organisation, who will come up with a plausible story to get you to share your financial/personal information. They can fake their telephone number and do some basic research online to get unique details about you to sound more convincing.

Social engineering: Fraudsters manipulate or trick people into exposing their personal or financial information, through fake emails, phone calls, text, posts on social media. These can be very complex attacks, some combining various sources of information about you to appear more convincing.

Phishing and smishing: Fraudsters send emails or text messages that appear to be from a genuine company. They typically ask you to make urgent contact via a telephone number within the text or via a website address, due to an unauthorised payment.

Online scams: Scammers advertise goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.

Money Mules: A "witting" mule assists the crime by providing the bank account where the proceeds of any fraud or scams can be paid to. Fraudsters and scammers can open an account themselves using fake ID, or can convince someone who already has a bank account to receive money on their behalf. By supplying the information, you also risk getting into trouble as you become complicit in the crime.

- Ask the group/individual to come up with their own fraud case studies. The examples on **Worksheet 3** can be used for inspiration if they are struggling to think of ideas. Use the following prompt questions to help them build their case study:

What type of fraud or practice is being demonstrated?

What signs could the person affected have spotted to stay safe?

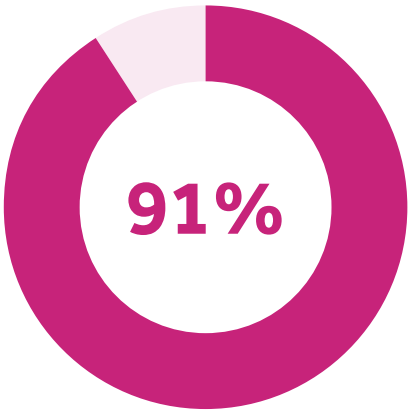
What could they do differently next time? Examples could include: not revealing personal or financial data, verifying whether links in emails are legitimate by contacting the company directly, not opening email attachments from unknown sources

- You can print **Worksheet 4** as a takeaway. You could end the session by showing a relevant film from getsafeonline.org/videos/

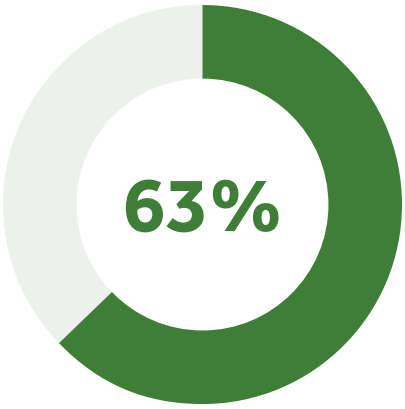
LifeSkills

Financial fraud, scams and identity theft

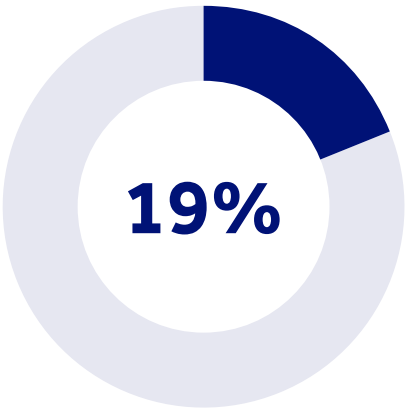
Worksheet 1: 2021 Identity theft stats



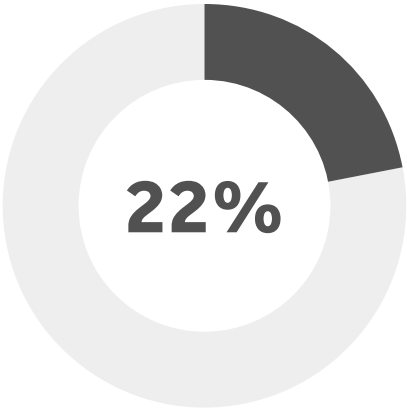
of identity fraud was committed online



of all fraud is identity theft



increase in identity theft among those under 21 since 2016



growth in identity fraud cases in 2021

LifeSkills

Financial fraud, scams and identity theft

Worksheet 2: Fraud terms

Vishing

A phone call from a fraudster posing as an employee of a reputable company or organisation, who will come up with a plausible story to get you to share your financial/personal information. They can fake their telephone number and do some basic research online to get unique details about you to sound more convincing.

Social engineering

Fraudsters manipulate or trick people into exposing their personal or financial information, through fake emails, phone calls, texts, or posts on social media. These can be very complex attacks, some combining various sources of information about you to appear more convincing.

Phishing and smishing

Fraudsters send emails or text messages that appear to be from a genuine company. They typically ask you to make urgent contact via a telephone number within the text or via a website address, due to an unauthorised payment.

Online scams

Scammers advertise goods or services that don't exist or aren't theirs to sell. They convince you to send the payment directly to their bank but the goods never arrive, or are not as advertised.

Money Mules

A "witting" mule assists the crime by providing the bank account where the proceeds of any fraud or scams can be paid to. Fraudsters and scammers can open an account themselves using fake IDs, or can convince someone who already has a bank account to receive money on their behalf. By supplying the information, you also risk getting into trouble as you become complicit in the crime.

LifeSkills

Financial fraud, scams and identity theft

Worksheet 3: Financial fraud, scams and identity theft in action

Case study 1

Priya had been looking for a job to earn some money, when she was approached outside her college by someone who offered her a way of making easy cash. They asked Priya to share her bank details so that money could be transferred into her account for a short period of time. She agreed when they said that whilst £500 would be transferred in, she would only have to transfer £450 and she could keep the rest.

Case study 2

Jake was keen to get tickets for a football match which had sold out. He found some advertised online cheaper than the original price, and paid for them using his debit card. Jake was sent a confirmation email straight away to say that the tickets would arrive within 10 days. Unfortunately, the tickets never arrived and when he made calls to the company they were ignored.

Case study 3

Tom got a text message from his mobile phone contract provider to say that his account had been used by someone else to download lots of apps. To get a refund, Tom was asked to click on a link and enter his bank details and the three-digital security code on his debit card into a form online; he was told that this refund would appear in his account within 5-10 days. The following day, when Tom checked his bank balance using his mobile banking app, he saw that a large sum of money had been withdrawn from his account.

LifeSkills

Financial fraud, scams and identity theft

Worksheet 4: Financial fraud, scams and identity theft summary

Top tips for staying digitally safe:

1. Check how much personal information is public on your social media accounts. Fraudsters can use information such as your birthday, home town, pet names, holiday dates, or job title to steal your identity and apply for bank accounts or buy products in your name
2. Never share your PIN, bank details or passwords with anyone who approaches you or contacts you through text, email, phone or in person, and don't write them down
3. Phone organisations directly from the number listed on their website to verify who is contacting you
4. Password protect your devices using random words and include symbols, numbers and capitals and regularly change them
5. Limit your online activity when using open public Wi-Fi connections, including logging on to your email, online banking and online shopping
6. Check the web address begins with 'https' and that there's an unbroken padlock symbol in the browser address bar, especially when online shopping. You can hover over links without clicking to see the destination
7. Install anti-virus software on your laptop and any other personal devices and keep it up to date

LifeSkills

Further support

The following links can be explored to get further advice on a number of topics around managing finances and living independently:

The Childrens Commissioner (general advice for those up to 25)
childrenscommissioner.gov.uk

The Rees foundation (general support for Care Leavers of any age)
reesfoundation.org

Care Leaver Covenant (help finding job opportunities)
mycovenant.org.uk

The Association of British Credit Unions (help finding the right credit unions and general information about these)
findyourcreditunion.co.uk

Propel (support for those going to university, including financial advice)
propel.org.uk/UK

Citizens Advice Bureau (general legal and financial advice)
citizensadvice.org.uk

Step Change (debt management advice)
stepchange.org

Money Helper (general financial advice)
moneyhelper.org.uk

Debt Advice Foundation (free, confidential debt advice charity)
debtadvicefoundation.org

Benefit calculator (free tool to help find estimates for benefits entitlements)
entitledto.co.uk/help/better-off-calculation

Experian (free tool for credit score checks)
experian.co.uk

If you are a young person and want to know more about money and work, register at https://barclayslifeskills.com/help-myself/

If you are working with young people who have experienced care, explore more adapted content at barclayslifeskills.com/help-others/lessons and select '**Care leavers'**.

Many other LifeSkills lessons are also suitable for use with care leavers to support them on their employability journey. To find out more, go to barclayslifeskills.com/help-others/lessons and select the **'Building key skills to do well at work'** category.